



3       receiving an authentication credential from the user;  
4       verifying that the authentication credential is valid; and  
5       providing the time-stamped token to the user-device, wherein the time-  
6       stamped token includes the authentication and a time.

1           5.       The method of claim 4, wherein determining if the authentication  
2   has expired involves:

3 recovering the time-stamped token from the user-device;  
4 adding the specified period to the time within the time-stamped token to  
5 produce an expiry time; and  
6 detecting if a current time is later than the expiry time, whereby if the  
7 current time is later than the expiry time, the authentication has expired.

1           6.       The method of claim 5, wherein the time within the time-stamped  
2   token is updated to the current time by a partner application when the partner  
3   application is accessed.

1           7.       The method of claim 4, wherein the time-stamped token is a  
2   domain cookie, wherein the domain cookie is accessible by multiple network  
3   servers within a domain on the public network.

1           8.       The method of claim 4, wherein the time-stamped token is  
2 encrypted to prevent attacks.

9. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method to facilitate global timeout in a distributed computing environment, the method comprising:

- receiving an access request from a user at an application in the distributed computing environment;
- determining if the distributed computing environment has issued an authentication to a user device through which the user accesses the application, wherein the authentication is stored within a time-stamped token on the user-device, and wherein the authentication has not expired; and
- if the authentication has not been received or has expired, redirecting the access request to a single sign-on server for the distributed computing environment;
- otherwise granting access to the application to the user.

10. The computer-readable storage medium of claim 9, wherein the distributed computing environment includes multiple partner applications distributed across multiple network servers coupled to a public network.

11. The computer-readable storage medium of claim 10, wherein the public network includes the Internet.

1           12.     The computer-readable storage medium of claim 10, wherein  
2     determining if the distributed computing environment has issued the  
3     authentication to the user involves:  
4             receiving an authentication credential from the user;  
5             verifying that the authentication credential is valid; and  
6             providing the time-stamped token to the user-device, wherein the time-  
7     stamped token includes the authentication and a time.

1           13.     The computer-readable storage medium of claim 12, wherein  
2     determining if the authentication has expired involves:  
3           recovering the time-stamped token from the user-device;  
4           adding the specified period to the time within the time-stamped token to  
5     produce an expiry time; and  
6           detecting if a current time is later than the expiry time, whereby if the  
7     current time is later than the expiry time, the authentication has expired.

1           14.     The computer-readable storage medium of claim 13, wherein the  
2     time within the time-stamped token is updated to the current time by a partner  
3     application when the partner application is accessed.

1           15.     The computer-readable storage medium of claim 12, wherein the  
2     time-stamped token is a domain cookie, wherein the domain cookie is accessible  
3     by multiple network servers within a domain on the public network.





1           23.     The apparatus of claim 20, wherein the time-stamped token is a  
2     domain cookie, wherein the domain cookie is accessible by multiple network  
3     servers within a domain on the public network.

1           24.     The apparatus of claim 20, wherein the time-stamped token is  
2     encrypted to prevent attacks.

10073089-020802